CLAIMS

1. A method of converting data between an unencrypted format and an encrypted format, wherein said data are organised in bit words, the method including a plurality of rounds, each round being comprised of fixed set of transformations applied to a two-dimensional array, designated the state, of rows and columns of bit words, the method including the step of applying at least a part of said fixed set of transformations to a transposed version of said state, wherein said rows and columns are transposed for the columns and the rows, respectively.

2. The method of claim 1, wherein said bit words are 8-bit words or bytes.

3. The method of claim 1, wherein said state is a 4x4 matrix of bit words.

4. The method of claim 1, including 10, 12 or 14 rounds.

5. The method of claim 1, wherein said rounds involve the use of respective round keys, and wherein said round keys are subjected to transposition before being used in a respective round applied on a transposed state.

6. The method of claim 5, wherein said round keys are applied according to a round key schedule, the method including the step of applying said round key schedule as in the case of rounds providing for said set of transformations being applied to a non-transposed state and the step of adding code to transpose every round key thus created.

7. The method of claim 1, including the step of applying said round keys according a transposed key schedule.

8. The method of claims 1, including the step of re-transposing said transposed state before outputting it.

9. A circuit for converting data between an unencrypted data format and an encrypted format, the circuit including registers for storing said data in the form of bit words as well as circuitry for implementing a plurality of rounds, each round being comprised of a fixed set of transformations applied to a two-dimensional array, designated the state, of rows and columns of bit words, wherein said circuitry is arranged to apply at least part of said fixed set of transformations to a transposed version of said state, wherein rows and columns are transposed for columns and rows, respectively.

10. The circuit of claim 9, wherein said registers are adapted for storing said bit words as 8-bit words or bytes.

11. The circuit of claim 9, wherein said circuitry is configured to operate on said state in the form of a 4x4 matrix of bit words.

12. The circuit of claim 9, wherein said circuitry is configures to implement 10, 12 or 14 rounds.

13. The circuit of claim 9, wherein said circuitry includes respective sets of S-box processing modules, each said set of S-box modules operating on a group of bit words corresponding to a cell of a column of said state.

14. The circuit of claim 13, wherein each said column is composed of four said cells.

15. The circuit of claim 9, including a plurality of respective sets of shift column modules each set being adapted to perform a column shift operation on a column of said state.

16. The circuit of claim 15, including a single mix column module to perform column mix operations on the shift column data generated from the shift column modules of said plurality.

17. The circuit of claim 9, wherein the circuit is an encoder for converting data from an unencrypted data format into an encrypted data format.

18. The circuit of claim 17, wherein the circuit is an embedded system such as an integrated circuit in a smart card.

19. The circuit of claim 9, wherein the circuit is a decoder for converting data from an encrypted data format into an unencrypted data format.

20. The circuit of claim 19, wherein the circuit is an embedded system such as an integrated circuit in a smart card.